Children's Internet Proctection Act

Introduction

The (CIPA) was signed into law on December 21, 2000. To receive support for Internet access and internal connections services from the Universal Service Fund (USF), school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. The relevant authority with responsibility for administration of the eligible school or library must certify the status of its compliance for the purpose of CIPA in order to receive USF support.

In general, school and library authorities must certify either that they have complied with the requirements of CIPA; that they are undertaking actions, including any necessary procurement procedures, to comply with the requirements of CIPA; or that CIPA does not apply to them because they are receiving discounts for telecommunications services only.

Requirements of CIPA

CIPA requirements include the following three items:

Technology Protection Measure

A technology protection measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors.

Internet Safety Policy

The Internet safety policy must address the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web

- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications

- Unauthorized access including "hacking" and other unlawful activities by minors online

- Unauthorized disclosure, use, and dissemination of personal information regarding minors

- Measures designed to restrict minors' access to materials harmful to minors

Public Notice and Hearing

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed technology protection measure and Internet safety policy.

INTERNET SAFETY POLICY
For <School>
Introduction
It is the policy of **<School>** to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions
Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material
To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.
Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.
Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage
To the extent practical, steps shall be taken to promote the safety and security of users of the **<School>** online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring
It shall be the responsibility of all members of the <School or Library> staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.
Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of <Title> or designated representatives.

Adoption
The Board of <School> adopted this Internet Safety Policy at a public meeting, following normal public notice, on <Month, Day, Year>.
CIPA definitions of terms:
TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;
2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or
3. Harmful to minors.
HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

On November 14 our school held a public meeting to introduce and explain CIPA. We also present internet safety meetings for parents and guardians in April of each year.